

# IRAN

	2009	2011
<b>INTERNET FREEDOM STATUS</b>	<b>Not Free</b>	<b>Not Free</b>
<b>Obstacles to Access</b>	21	21
<b>Limits on Content</b>	24	29
<b>Violations of User Rights</b>	31	39
<b>Total</b>	<b>76</b>	<b>89</b>

**POPULATION:** 75.1 million

**INTERNET PENETRATION 2009:** 11 percent

**WEB 2.0 APPLICATIONS BLOCKED:** Yes

**SUBSTANTIAL POLITICAL CENSORSHIP:** Yes

**BLOGGERS/ONLINE USERS ARRESTED:** Yes

**PRESS FREEDOM STATUS:** Not Free

## INTRODUCTION

Since the protests that followed the disputed presidential election of June 12, 2009, the Iranian authorities have waged an active campaign against internet freedom, employing extensive and sophisticated methods of control that go well beyond simple content filtering. These include tampering with internet access, mobile-telephone service, and satellite broadcasting; hacking opposition and other critical websites; monitoring dissenters online and using the information obtained to intimidate and arrest them; ordering blogging service providers inside Iran to remove “offensive” posts or blogs; and trying to fill the information vacuum created by these measures with propaganda and misinformation.

The Iranian regime has long had an ambivalent relationship with the internet, viewing it alternately as a catalyst for economic development and diversification or as an invading force that threatens the state’s strict social, religious, and political values. The internet was first introduced by the government in the 1990s to support technological and scientific progress in an economy that had been deeply affected by eight years of war with Iraq. However, until 2000, the state played an insignificant role in the growth of internet use among the Iranian public. In this period the private sector was the main driver of internet development, leaving the state with the challenging task of keeping up with a dynamic and overwhelmingly youthful society. The government of the reformist president Mohammad Khatami (1997–2005) then invested heavily in expanding the internet infrastructure, but during his administration, the authorities began to clamp down on free expression in both the traditional media and online.

Supreme Leader Ali Khamenei first asserted control over the internet through a May 2001 decree and subsequent legislation by the Cultural Revolution High Council that forced all internet service providers (ISPs) to end their direct connections, obtain a license to operate, and purchase their bandwidth from government-controlled Access Service Providers.<sup>1</sup> The regime's ferocious attacks on internet use after the 2009 election seemed to mark the end of its internal debate, as the leadership decisively chose political control over the benefits of a more open society.

## OBSTACLES TO ACCESS

The Khatami administration, following an economic development plan devised during the last term of President Akbar Hashemi Rafsanjani, worked to connect different cities with fiber-optic cables and increase the Iranian internet's connection points to the global network. The result of this and other such efforts was an explosion in internet use in the country. According to the International Telecommunication Union (ITU), there were 625,000 internet users in Iran at the beginning of 2000. By the end of Khatami's presidency in 2005, the number had increased to several million. This period also featured a major demographic shift in Iran. The population had increased tremendously since the end of the Iran-Iraq war, to a point where more than 70 percent of the population was born after the 1979 revolution. Faced with restrictions on most other forms of expression and social interaction, this young population turned to the internet in large numbers. At the same time, the cost of internet access remains very high and the service is mostly available in the cities, meaning users are predominantly urban middle and upper class. A report prepared by Iran's parliament blames the government for holding a monopoly on internet bandwidth and selling it to users through a number of intermediaries.<sup>2</sup> Direct access to the internet via satellite is only permitted to certain institutes, and it remains prohibited for personal use.

Statistics relating to the number of internet users in Iran are inconsistent and highly disputed, even among Iranian officials. The single official source of data is the ITU, which receives statistics from the government on different information and communications technology (ICT) indicators. According to official sources, the Iranian government calculates the number of internet users by forecasting the number of potential users based on the available bandwidth. Therefore, the reported numbers do not correspond to the actual number of Internet users at all. According to a survey conducted in 2009 by Iran Statistics Centre and published in March 2010, the internet penetration rate in Iran stood at 11 percent; 30 percent of the internet users were based in Tehran; and the penetration rate was

<sup>1</sup> "Country Profile—Iran," OpenNet Initiative, June 16, 2009, <http://opennet.net/research/profiles/iran>.

<sup>2</sup> Iran ICT News, "Identifying the causes behind the expensiveness of the Internet in Iran," October 10, 2010, <http://tinyurl.com/33vpzjf>.

15 percent in urban and 3 percent in rural areas. This is significantly lower than the internet penetration reported to the ITU the same year, which was approximately 38 percent.<sup>3</sup>

The internet and its users played an important role in the opposition movement following the June 2009 presidential election, in which incumbent Mahmoud Ahmadinejad was accused of winning a new term through fraud. After the authorities barred international media from directly covering the opposition protests and ensuing violence by security forces, foreign outlets came to rely on user-generated content posted on the internet from inside Iran. The regime characterized these interactions between protesters, internet users, and international media as a “soft war” orchestrated by foreign powers, and vowed to combat it in kind. The government has reportedly allocated \$500 million in its 2010–11 annual budget for this purpose.

During the protests, authorities curbed internet access by introducing 60 to 70 percent packet loss into the network, resulting in a massive drop in speed.<sup>4</sup> This came in the context of an existing 128-kilobyte bandwidth limitation imposed on private broadband users beginning in 2006.<sup>5</sup> By March 2009, there were only around 557,857 broadband subscribers in Iran, the majority of private users are connected with 56kb to the internet.<sup>6</sup> Given these obstacles, it became difficult to conduct basic online activities like opening e-mail messages or viewing simple webpages.<sup>7</sup> The government blamed the slowdown on damage to undersea cables in the Persian Gulf, but the timing was very much aligned with key protests, which strongly suggests that the authorities were in full control of internet speed. Similarly, during protest days many of the important network ports used by instant-messaging and chat platforms were also tampered with, resulting in partial or complete loss of function for these tools.

As of December 2010, all the major international social-networking and media-sharing websites like Facebook, YouTube, and Flickr were blocked, while some file types, such as MP3 audio files, have been sporadically filtered. The periodic filtering and disruption of services based overseas—such as Google’s fairly well-encrypted e-mail and blogging platforms, Gmail and blogger.com—appear designed to frustrate users and eventually force them to seek more easily monitored alternatives based in Iran. Although many Iranians have been able to access the blocked platforms and content by using various circumvention techniques, the authorities have actively worked to disrupt such efforts, forcing users to constantly adapt and search for new solutions.

---

<sup>3</sup> Editor’s note: After publication of this report, the ITU revised its internet penetration figure for Iran from 38 percent to 11 percent.

<sup>4</sup> Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination.

<sup>5</sup> “Iranian Government: Internet Speed is Good” (in Persian), BBC, May 21, 2010 [http://www.bbc.co.uk/persian/iran/2010/05/100521\\_138\\_iran\\_internet\\_speed\\_taghipour.shtml](http://www.bbc.co.uk/persian/iran/2010/05/100521_138_iran_internet_speed_taghipour.shtml).

<sup>6</sup> The association of private broadband service providers in Iran, “official stats on available broadband ports in Iran until March 19, 2010” <http://www.adsl-pap.com/fa/port/>.

<sup>7</sup> It takes 6 minutes to download a MP3 music file with 128kb connection and 12 minutes with 56kb connection.

According to official statistics, there are approximately 54 million mobile-phone subscriptions in Iran. Mobile-telephone service was also subject to government controls. Mobile-phone text messaging, or short-message service (SMS), was shut down throughout Iran the day before the election and did not resume until 40 days later. Subsequently it was disrupted on a temporary basis immediately before and during key protests days. There have been reports that messages with banned keywords were filtered even when service was up. However, any use of SMS by dissenters in Iran is very limited and highly risky. Users must present some form of identification when purchasing mobile-phone subscriptions, making it an easy task for the authorities to track down the authors and recipients of specific messages.

The period after the election featured a broad assertion of power by the Islamic Revolutionary Guards Corps (IRGC), a politically important branch of the security forces that also controls large sections of the economy. Even as it managed the government's crackdown in the streets, it used its economic muscle to increase state dominance of the information landscape. In September 2009, for example, the IRGC purchased a controlling stake in the Telecommunication Company of Iran (TCI), the country's main provider of internet and mobile-telephone service. The second mobile operator, IranCell, is owned in part by a web of proxy companies controlled by the IRGC (there are a number of high profile IRGC ex-commanders among its management). The third operator, due to be launched in early 2011, is a government-owned entity.

## LIMITS ON CONTENT

Internet filtering, which began toward the end of the Khatami presidency in 2005, has become more severe since the June 2009 election. The authorities now employ a centralized filtering system that can effectively block a website within a few hours across the entire network in Iran. Private internet-service providers (ISPs) were forced to either use the bandwidth provided by the government or route their send traffic (which contains the site-visit requests) through government-issued filtering boxes developed by software companies inside Iran. The boxes work by searching for banned text strings—either keywords or domain names—in the URL requests submitted by users.

In recent years there has been pressure within the Iranian government to show that the filtering of content is based on a legal framework and is not arbitrary. As a result, institutions in charge of internet filtering have evolved. In July 2009, Ahmadinejad's government enacted the Computer Crime Law, which had been passed by the parliament a year earlier. According to this law, the Committee in Charge of Determining Unauthorized Websites is legally empowered to identify sites that carry forbidden content and report that information to TCI and other major ISPs for blocking. The committee is headed by the prosecutor general and operates under the supervision of his office. The rest of the panel

consists of representatives from 12 governmental ministries and institutes. The law also identifies the violations that might result in a website being marked for filtering. These are defined very broadly and cover a variety of topics, ranging from insulting religious figures and government officials to distributing pornographic content and illegal circumvention tools.

Little information is available about the inner workings of the committee. According to the law it should meet biweekly to decide on any website bans, but a TCI vice president recently put the rate of filtering at 200 to 300 websites per day, meaning the bulk of filtering decisions are likely made automatically upon discovery of objectionable content, or by a small technical group in charge. This would leave the committee to decide on only the more controversial blocking decisions, such as the move during the protests to block the website of the Combatant Clergy Association (Majmae Rohanion Mobarez), a pragmatic-conservative clerical party linked to Rafsanjani. The official websites of Khatami and a number of Grand Ayatollahs who have criticized the government were also blocked. As the head of two important state bodies, the former president remained an influential member of the establishment, but he had been Ahmadinejad's electoral opponent in 2005, and he sometimes appeared to side with the opposition in 2009.

There have been other cases of filtering aimed at websites that operate within the official discourse. A number of websites and blogs belonging to Ahmadinejad supporters who publicly criticized some of his government's policies were also blocked. In such an environment, any website that includes elements of opposition discourse is bound to be targeted. The opposition Green Movement, other political groups, women's rights groups, ethnic and religious minorities, and the Iranian homosexual community fall within the category of opposition discourse and are affected by heavy filtering. In addition to blocking certain content, the Computer Crime Law makes service providers, such as blogging platforms, responsible for any content that appears on their sites. This has led to the suspension of a number of blogs hosted on platforms inside Iran.

The authorities claim that there is a procedure for disputing filtering decisions. However, the procedure is highly inefficient, even for a prominent conservative blogger, Omid Hosseini-Ahdestan, whose site was filtered "accidentally." He did not succeed in unblocking his blog through the complaint procedure, but the filter was lifted after high-profile media coverage of the incident.<sup>8</sup> The dispute process requires the website owner to disclose his or her personal information and accept responsibility for any misconduct in the future, a commitment that few are willing to make given the risk of severe punishment.

In addition to censorship, the state counters critical content and online organizing efforts by extending state propaganda into the digital sphere. There are at least 400 news websites that are either directly or indirectly supported by the state. They seek to set the

---

<sup>8</sup> Ahdestan blog, "On filtering of Ahdestan", January 15, 2010.  
<http://ahdestan.wordpress.com/2010/01/15/ahdestan>.

agenda by providing partial commentary or publishing rumors. There have also been a large number of government-backed initiatives to promote blogging among supporters of government and members of the Basij paramilitary group. And during the postelection protests, there were reports of fake user-generated content submitted to Twitter and YouTube by government supporters to mislead the protesters and reporters. Some commentators have argued that propaganda is displacing censorship as the primary means of controlling the internet.<sup>9</sup>

Self-censorship is also very extensive, particularly on political matters. The widespread arrests of reporters and activists after the election, as well as perceptions of pervasive surveillance, have created fear among online journalists and bloggers. Many of them either abandoned their online activities or were forced to use pseudonyms. At least 1,500 bloggers who were blogging on political issues with their real identity decided to end their blogs or avoid writing about politics directly in the aftermath of the 2009 election. Furthermore, the majority of independent content producers lack the financial resources to operate in such a hostile environment. The online advertising market in Iran is exclusively limited to apolitical and pro-government websites. Even businesses based outside Iran avoid political websites to maintain trading relationships with the country. Due to international sanctions against Iran, Google Advertising does not recognize Persian as one of the languages in its advertising system, disadvantaging Persian content producers.

Despite all of these limitations, the internet remains the only means available for Iranian citizens and dissenters to get news and organize themselves. Iranian broadcast outlets are tightly controlled by the authorities, and satellite broadcasting from outside Iran is subjected to heavy jamming. The technical difficulty of engaging in similarly comprehensive censorship of a medium as complex and heavily populated as the Iranian internet may explain the authorities' growing reliance on propaganda, misinformation, and physical coercion to counter internet-based activism.

## VIOLATIONS OF USER RIGHTS

Iranian internet users suffer from routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those who are more critical of the authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly defined. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical

<sup>9</sup> Evgeny Morozov, "Iran's Propaganda Hits the 'Spinternet,'" CNN, December 29, 2009, <http://edition.cnn.com/2009/OPINION/12/29/morozov.dicatorships.internet/index.html>.

opinions. The Computer Crime Law passed by the parliament in 2008 and introduced officially by Ahmadinejad in July 2009 clearly identifies punishments for spying, hacking, piracy, phishing, libel, and publishing materials that are immoral and against public taste.

Since June 2009 the authorities have been cracking down on online activism through various forms of judicial and extrajudicial intimidation. An increasing number of bloggers have been threatened, arrested, tortured, kept in solitary confinement, and denied medical care, while others have been formally tried and convicted. At least 50 bloggers and online activists have been arrested, and a dozen are still being detained. They include 18-year-old Navid Mohebbi, who was arrested in September 2010 and then released conditionally in December after receiving a three-year suspended prison sentence on charges of “actions against national security” and insulting the Islamic Republic’s founder and current leader by means of “foreign media.” Another blogger Omidreza Mirsayafi died under questionable circumstances in Tehran’s infamous Evin prison. He was arrested in the aftermath of the election for allegedly insulting Iran’s religious leaders and conspiring against the government. A large number of bloggers, journalists, and activists have also fled Iran and sought political asylum in neighboring countries, mainly Turkey.

The Iranian authorities have taken a range of measures to monitor online communications and use them as a basis for criminal punishment. A number of protesters who were put on trial after the election were indicted for their activities on Facebook and Balatarin, a Persian site that allows users to share links and news. Many arrested activists reported that interrogators had confronted them with copies of their e-mails, asked them to provide the passwords to their Facebook accounts, and questioned them extensively on their relationships with individuals on their “friends” list. The authorities actively exploited the fear created by these reports, claiming that they had access to all the e-mail and text messages exchanged in Iran. The Computer Crime Law obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to monitor all this data. In addition, ISPs have been accused of forging SSL certificates to eavesdrop on emails sent through secure channels (https), making protected communication increasingly difficult for those without more sophisticated skills.

Explicit filtering and physical intimidation is supplemented by hacking and denial-of-service (DoS) attacks on the websites of government critics, including leading opposition figures. In the days after the disputed presidential election, many of the news websites set up by supporters of opposition candidates Mir Hossein Mousavi and Mehdi Karoubi were taken offline through arrests of the technical teams involved in their maintenance and through intense DOS attacks. There is technical evidence, including a log of the web servers,

confirming that government-owned internet-protocol (IP) addresses were used to launch attacks on opposition websites.<sup>10</sup>

Websites were rendered either permanently or temporarily unavailable by means of hacking. A group calling itself the Iranian Cyber Army managed to hack a number of opposition and news sites with a mix of technical methods and forgery. In some cases the hacking resulted in total discontinuity of the websites. One outlet so affected was MowjCamp.com, a popular site launched after the election that very soon became the main news website of the Green Movement. Outlets that were temporarily disabled by hacking included the Amsterdam-based Radio Zamaneh and the Jaras Green Movement website. A number of non-Iranian sites, such as Twitter, were targeted through the temporary hijacking of their domain names. At the time of these hacking incidents, there was speculation about the connection between the Iranian Cyber Army and the Iranian authorities. Some months later, Iranian officials confirmed these suspicions by publicly announcing that the Iranian Cyber Army was under the command of the IRGC.<sup>11</sup>

---

<sup>10</sup> Norooz News, “Norooz is revealing the names of 4 governmental entities behind the attacks against reformist websites,” October 17, 2010.

<sup>11</sup> Fars News, “IRGC has formed the second cyber army in the world,” May 20, 2010, <http://www.farsnews.com/newstext.php?nn=8902300353>.